REMARKS

The paragraphs starting at page 5, line 17, page 7, line 3, page 7, line 16, page 7, line 21, page 7, line 30, page 18, line 20, page 19, line 1, page 19, line 20, page 21, line 28, page 24, line 11, page 26, line 19, page 27, line 12, and page 28, line 22 in the specification have been amended to correct typographical errors. No new matter has been added.

Claims 1-59 are pending, with claims 1, 15, 16, 21 and 22 being independent. Claims 23-59 have been added.

Attached is a marked-up version of the changes being made by the current amendment.

Applicant asks that all claims be examined. Enclosed is a $666.00 check for excess claim fees. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: May 20, 2002

Scott R. Boalick
Reg. No. 42,337

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

Version with markings to show changes made

In the specification:

Paragraph beginning at page 5, line 17 has been amended as follows:

Referring to Fig. 2, the communications system 200 is an expansion of the block diagram of Fig. 1, focusing primarily on one particular implementation of the host system 20. The host system 20 includes a host device 22 and a controller 24. The host controller 24 generally is capable of transmitting instructions to any or all of the elements of the host device 22. For example, in one implementation, the host controller **[23]** 24 includes one or more software applications loaded on the host device 22. In other implementations, the host controller 24 may include any of several other programs, machines, and devices operating independently or collectively to control the host device 22.

Paragraph beginning at page 7, line 3 has been amended as follows:

In the implementation shown by Fig. 2, the OSP host complex 230 includes a routing processor 232. In general, the routing processor 232 will examine an address field of a data request, use a mapping table to determine the appropriate destination for the data request, and direct the data request to the appropriate destination. More specifically, in a packet-based implementation, the client system 10 may generate information requests, convert the requests into data packets, sequence the data packets, perform error checking and other packet-switching techniques, and transmit the data packets to the routing processor 232. Upon receiving data packets from the client system 10, the routing processor 232 may directly or indirectly route the data packets to a specified destination within or outside of the OSP host complex 230. For example, in the event that a data request from the client system 10 can be satisfied locally, the routing processor 230 may direct the data request to a local server **[234]** 236. In the event that the data request cannot be satisfied locally, the routing processor 232 may direct the data request externally to the Internet 30 or the IM host complex 220.

Paragraph beginning at page 7, line 16 has been amended as follows:

The OSP host complex 230 also includes a proxy server **[236]** 234 for directing data requests and/or otherwise facilitating communication between the client system 10 and the Internet 30. The proxy server **[236]** 234 may include an Internet Protocol ("IP") tunnel for converting data between an OSP protocol and standard Internet protocol to enable the client system 10 to communicate with the public Internet 30.

Paragraph beginning at page 7, line 21 has been amended as follows:

The proxy server **[236]** 234 also may allow the client system 10 to use standard Internet protocols and formatting to access the OSP host complex 230 and Internet 30. For example, the subscriber may use an OSP TV client application having an embedded browser application installed on the client system 10 to generate a request in standard Internet protocol, such as HyperText Transport Protocol ("HTTP"). In a packet-based implementation, data packets may be encapsulated inside a standard Internet tunneling protocol, such as, for example, User Datagram Protocol ("UDP") and routed to the proxy server **[236]** 234. The proxy server **[236]** 234 may include **[an]** a Layer Two Tunneling Protocol ("L2TP") tunnel capable of establishing a point-to-point protocol ("PPP") session with the client system 10.

Paragraph beginning at page 7, line 30 has been amended as follows:

The proxy server **[236]** 234 also may act as a buffer between the client system 10 and the Internet 30, and may implement content filtering and time saving techniques. For example, the proxy server **[236]** 234 can check parental controls settings of the client system 10 and request and transmit content from the Internet 30 according to the parental control settings. In addition, the proxy server **[236]** 234 may include one or more caches for storing frequently accessed information, or may enable access to similar caches stored elsewhere. If requested data is determined to be stored in the caches, the proxy server **[236]** 234 may send the information to the client system 10 from the caches and avoid the need to access the Internet 30.

Paragraph beginning at page 18, line 20 has been amended as follows:

After one or more digital images are received (step 510), a first storage facility for storing a digital image is identified (step 515). In general, the host system 20 identifies a first storage facility for storing a digital image. In one implementation, the host system 20 includes an image storage server system 2410 having a plurality of image storage servers 2412 configured to store digital images. The host system 20 further includes a film handler 242 that identifies one of the plurality of image storage servers 2412 as being available to store a digital image. For example, the film handler 242 may access a configuration file that contains a complete list of image storage servers 2412 and selects particular image storage servers 2414 in round-robin fashion. After selecting a particular image storage server 2412, the film handler 242 may communicate with the image write server 2414 and confirm that the image storage **[sever]** server 2412 is capable of storing the digital image.

Paragraph beginning at page 19, line 1 has been amended as follows:

After the first storage facility has been identified (step 515), a directory within the first storage facility is identified for storing a digital image (step 520). In general, the host system 20 identifies a directory in the first storage facility. In one implementation, the host system 20 includes a plurality of image storage servers **[2414]** 2412, each image storage server **[2414]** 2412 having a directory structure for storing digital images. Typically, the directory structure for an image storage server 2412 will include several tiers identifying the storage facility, a directory, and several subdirectories. The host system 20 may include a film handler 242 that identifies one of the plurality of directories within a particular image storage server 2412 as being available to store a digital image. For example, the film handler 242 may access a configuration file that contains a complete list of first tier directories associated with each image storage server 2412. The film handler 242 may select particular first tier directories in the image storage server **[2414]** 2412 in round-robin fashion. After selecting a particular first tier directory, the film handler 242 may communicate with the image write server 2414 and confirm that the particular image storage **[sever]** server 2412 is capable of storing the digital image within the particular first tier directory.

Paragraph beginning at page 19, line 20 has been amended as follows:

After a particular directory with the storage facility has been identified (step 520), a first image identifier is generated (step 525). In general, the host system 20 generates a first image identifier associated with the identified storage facility and directory. In one implementation, the host system 20 includes an image write server 2414 that generates a first image identifier corresponding to the identified storage facility and directory. One example**[,]** of a first image identifier is an 8 hexadecimal (32 bit) character string in which the first three hexadecimal characters correspond to the storage facility, the next three hexadecimal characters correspond to the directory, and the last two hexadecimal characters correspond to an encryption method. Typically, the groups of hexadecimal characters corresponding to the storage facility, directory, and encryption are coded. To illustrate, an example of a first image identifier (image_id_pl) is FEDCBA98. The characters FED correspond to a particular storage facility, for example, the image storage server 2412 named ygppics-d01.blue.isp.com. In this illustration, the characters CBA correspond to a directory within the particular image storage facility, for example, the main storage directory 010. The characters 98 correspond to an encryption method, for example, the MD5 algorithm or DEC algorithm.

Paragraph beginning at page 21, line 28 has been amended as follows:

Identifying the storage path may involve translating the extracted path information using a decoder (e.g., a look up table). For example, the decoder may translate the host characters FED into the **[sever]** server name ygppics-d01.blue.isp.com, the AAA characters CBA into the main directory 101, the BB characters 76 into the first subdirectory 05, the CC characters 54 into the second directory 72, the DD characters 32 into the third subdirectory FA, and the EE characters 10 into the fourth subdirectory CB.

Paragraph beginning at page 24, line 11 has been amended as follows:

Providing access to digital images and metadata describing the digital images may include allowing subscribers to view one or more digital images. In general, the film and image tables 2406 are searchable by various criteria (e.g., primary keys) including screen name. For example, by passing a subscriber's screen name to the film and image tables 2406, the account manager 244 can retrieve image records and/or film records associated with the subscriber's account. Typically, the retrieved records will include image identifiers referencing one or more stored digital images. The account manager 244 can use the image identifiers (e.g., image_id_p1 and image_id_p2) to determine the storage path of a particular digital image stored in a particular image storage server 2412 within the image storage server system 2410, as described above. By navigating to the appropriate storage path in the image storage **[sever]** server system 2410, the account manager 244 can retrieve and display a particular digital image to a subscriber.

Paragraph beginning at page 26, line 19 has been amended as follows:

Within a very short period of time (e.g., 5 minutes) after the notification is received **[generated]**, a storage location associated with the complaining subscriber is identified (step 615). In general, the host system 20 identifies an appropriate database (e.g., image farm database 2404) containing metadata associated with the complaining subscriber. Identifying the appropriate**[d]** database may include determining a storage space group containing the appropriate image farm database 2404 from account information associated with the complaining subscriber. For example, the account name (e.g., screen name) associated with the complaining subscriber may be encoded using a proprietary OSP hashing code. In one implementation, the monitoring system 246 applies the same proprietary hashing code to the subscriber's screen name as described above and is mapped by the distribution server 2402 to the appropriate storage space group, i.e., bucket, containing the image farm database 2404.

Paragraph beginning at page 27, line 12 has been amended as follows:

Then, a storage location associated with the owner of the offending digital image is identified (step 625). In general, the host system 20 identifies an appropriate database (e.g., image farm database 2404) containing metadata associated with the owner of the offending digital image. Identifying the appropriate**[d]** database may include determining an account name (e.g., screen name) associated with the owner of the offending digital image. The owner's screen name may be obtained from the film reference table 2406a in the complaining subscriber's bucket, for example. Identifying the appropriate database also may include determining a storage space group containing the appropriate image farm database 2404 from account information associated with the complaining subscriber. For example, the account name (e.g., screen name) associated with the offending digital image may be encoded using a proprietary OSP hashing code. In one implementation, the monitoring system 246 applies the same proprietary hashing code to the owner's screen name as described above and is mapped by distribution server 2402 to the appropriate storage space group, i.e., bucket, containing the image farm database 2404.

Paragraph beginning at page 28, line 22 has been amended as follows:

Then, the offending digital image is retrieved (step 640). In general, the host system 20 retrieves the offending digital images. In one implementation, the host system 20 includes a monitoring system 246 configured to navigate to the appropriate storage path in the image storage **[sever]** server system 2410.

In the claims:

Claim 1, 11, and 14-16 have been amended as follows:

1. A method of storing digital images within a computer system comprising:

identifying a first storage facility and a directory within the first storage facility for storing a digital image;

generating a first image identifier associated with the first storage facility and the directory;

generating a second image identifier comprising a random number;

generating a unique hash value by encrypting the first and second image identifiers; and

identifying a storage path using the first and second image identifiers and the unique hash value such that related digital images have unrelated storage paths.

11. The method of claim 9 further comprising mapping the encoded account information to an appropriate storage space group containing the second storage facility.

14. The method of claim 1 wherein gathering the unique hash value comprises applying at least **[on]** one of the MD5 algorithm and the DEC algorithm to the first and second image identifiers.

15. A digital image storage apparatus, comprising a host configured to:

identify a first storage facility and a directory within the first storage facility for storing a digital image;

generate a first image identifier associated with the first storage facility and the directory;

generate a second image identifier comprising a random number;

generate a unique hash value by encrypting the first and second image identifiers; and

identify a storage path using the first and second image identifiers and the unique hash value such that related digital images have unrelated storage paths.

16. A computer program, stored on a computer readable medium, comprising instructions for:

identifying a first storage facility and a directory within the first storage facility for storing a digital image;

generating a first image identifier associated with the first storage facility and the directory;

generating a second image identifier comprising a random number;

generating a unique hash value by encrypting the first and second image identifiers; and

identifying a storage path using the first and second image identifiers and the unique hash value such that related digital images have unrelated storage paths.